Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of:	)	
	)	
Cyber Security Certification Program	)	**PS Docket No. 10-93**
	)	
	)	
	)	
	)	
	)	

COMMENTS ON NOTICE OF INQUIRY

TELCORDIA TECHNOLOGIES

Telcordia Technologies (Telcordia) hereby submits comments to the Federal Communications Commission (FCC or "Commission") on its Notice of Inquiry (NOI) requesting Comments on a Cyber Security Certification Program in the above-captioned proceeding.[1] The Notice seeks comments on whether the Commission should establish a voluntary program under which participating communications service providers[2] would be certified by the FCC or a yet to be determined third party entity for their adherence to a set of cyber security objectives.

The Commission seeks comment on the components of such a program, if any, and whether such a program would create business incentives for providers of communications services to sustain a high level of cyber security culture and practice. It is the FCC's goal to promote security awareness, create a security baseline for

[1] Notice of Inquiry "Cyber Security Certification Program," Public Safety No. 10-93, FCC 10-63, Released April 21, 2010.

[2] By the term "communications Service provider," the Commission means an entity that provides communications service by radio, wire, cable, satellite and/or lightguide for a fee to one or more unaffiliated entities. *See,* NOI, at fn1.

telecommunications networks and components, and bring all industry stakeholders up to this baseline level in the not too distant future.

BACKGROUND

Telcordia is a software, engineering and consulting company with a vested interest in advancement of telecommunications security. Telcordia, formerly known as Bell Communications Research (Bellcore), was created in 1984 at the time of the AT&T divestiture as a unique entity with a mission to provide common R&D as well as technology generic requirements and seamless operational capabilities across all the new service provider boundaries. Telcordia's charter includes technical and management support to protect the integrity and interoperability of the telecommunications infrastructure and, as such, we have worked actively with government and industry in the area of national security and emergency preparedness (NS/EP). Telcordia is vendor neutral and technology agnostic and possesses the depth and breadth of telecommunications experience to handle the full spectrum of broadband and information network engineering and design issues. We offer the following comments on the issues raised by the Commission.

DISCUSSION

Increasing Complexity in Infrastructure, Services, and Threats

The deployment of Next Generation Networks (NGNs), mobile and distributed networking, Peer-to-Peer (P2P) communications, and third party-developed applications has redefined the technology foundation and changed the business dynamics of the telecommunications industry. The combination of emerging packet-based networks, advanced services, and more varied and intelligent devices supports a wider range of flexible, customized, and multimedia services. In addition to this fast-paced change in technologies and services, the entire concept of interconnection has evolved to include not just service provider-to-service provider, but also service provider-to-clouds and service provider-to-large enterprises. All of these types of interconnection and access arrangements, as well as ever smarter devices and advanced services, serve to increase available avenues for attack through both traditional and emerging vulnerabilities.

The complex and dynamic nature of our telecommunications industry is matched by an equally complicated and fast-changing threat environment. Cyber attacks include everything from spam and denial of service, to identity theft, malware, unauthorized data access, viruses, botnets, and cyber warfare. This expanding threat environment is driven in no small part by the expansion of the use of broadband and internet communications to support all areas of business and society. In some sense, the more ubiquitous and critical communications infrastructure becomes, the more attractive a target it is for mischief and malice. The baseline cyber security criteria will need to have the breadth, depth, and flexibility to address the complex technical, operational and business dimensions while providing protection against the evolving threats. The remaining sections of this Discussion address some aspects of this challenge in more detail.

Development of Baseline Security Criteria

As noted in a previous Telcordia comment, [3] there have been considerable and successful efforts over many years by the industry and standards bodies to improve the

[3] Telcordia's response to the National Broadband Plan Comment #8 on "Public Safety, Homeland Security and Cyber Security Elements," Public Notice DA 09-2133, submitted in November, 2009.

security of broadband telecommunications, including the development of a number of valuable and applicable security criteria.[4] Standards such as the NIST Special Publications 800 Series[5] risk management framework and the ISO 27002[6] security management standard are important examples. Another example is ongoing work in the 3GPP standards body defining the security architecture for Long Term Evolution (LTE) Fourth Generation mobile services.[7] However, the challenge will be to capture the various and diverse criteria developed by government, industry and international sources and meld them into a comprehensive risk-based criteria to address the changing technology and services, the different business models, the evolving threats and vulnerabilities, and the customer expectations for privacy, service availability, and transaction integrity. Appropriately selecting from these resources and augmenting as necessary will enable timely progress to be made on baseline security criteria. The FCC must fully recognize, however, that some of the existing cyber security standards and best practices are Information Technology (IT) centric and need to be expanded to address the various dimensions (e.g., signaling) of telecommunications environments.

Telcordia agrees with the FCC's concept of establishing a meaningful baseline of security capabilities for acceptance across the industry. Further, we believe that the complexity and diversity of the telecommunications infrastructure requires additional

[4] We note that Telcordia has a long history in contributing to the development of telecommunications security criteria; one example is the Generic Requirements document GR-815 (for Network Element/Network system (NE/NS) Security, GR-815-CORE, March 2002) which provides security requirements for telecommunications network elements.

[5] http://csrc.nist.gov/publications/PubsSPs.html.

[6] http://www.27000.org/iso-27002.htm.

[7] 3GPP TS 33.401 V8.1.1, System Architecture Evolution (SAE): Security Architecture, Release 8

criteria depending upon the specific technologies employed by the service provider. There are several ways to structure risk tiers above the baseline security criteria. Telcordia suggests that the most meaningful way to structure security criteria levels is by the technology type of the service provider because this will more closely match the complexities of the different technologies and functional domains deployed.

The FCC will need to work with the industry to jointly develop a comprehensive set of acceptable security criteria, as well as a criteria update process and an evaluation process. The effort will need to be a cooperative process involving public-private collaboration as the private sector will play crucial roles in developing and implementing any such program. Over the years, government and industry have collaborated to address similar areas related to security and reliability in groups such as NSTAC[8] and NRIC[9] (now replaced with CSRIC[10]). These collaborations provide working models the FCC can adapt to address cyber security for telecommunications. Further, we recommend the FCC consider exploring venues such as ATIS[11] as the incubator for its security standards, criteria and guidelines initiative because of its industry acceptance, wide participation, open and well honed processes and its successful past performance.

Need for Trained Telecommunications Security Professionals

In this NOI the Commission identified four initial important security areas: 1) secure equipment management, 2) updating software 3) intrusion prevention and

[8] National Security Telecommunications Advisory Committee

[9] Network Reliability and Interoperability Council

[10] Communications Security, Reliability and Interoperability Council

[11] Alliance for Telecommunications Industry Solutions

detection and 4) intrusion analysis and response. We agree that these four areas are significant, but would propose a 5th area – human resources – which is cross-cutting in nature and provides a foundation for all security work. We believe this 5th area is critical to the success of security improvement and should be given equal emphasis in the industry and in the FCC's efforts going forward. Irrespective of the emergence of new technologies and the success of security criteria and programs, it is critical to have skilled personnel to interpret test results and to assess subtle abnormalities in the environment. In some ways, having an adequately-sized workforce of trained, experienced individuals may be the single most important Critical Success Factor in the planning, design, building and operation of cyber security programs.

As with the previous discussion on baseline security criteria, existing programs for certifying security professionals are available which can provide valuable models for the telecommunications industry. One relevant example is the CISSP[12] offered by the International Information Systems Security Certification Consortium (ISC)^2. This program was recently recognized by SC Magazine as the "Best Professional Certification Program" for 2010.[13] Among the attractive features of the CISSP program are its global reach and acceptance and the program components that address the updating of professionals' knowledge. A second example is the Global Information Assurance

[12] Certified Information Systems Security Professional.

[13] See SC Magazine, March 2, 2010 at http://www.scmagazineus.com/best-professional-certification-program/article/164155/ which describes this gold-standard of information security certifications as follows: "The CISSP is not only an objective measure of excellence, but a globally recognized standard of achievement. It requires at least five cumulative years of relevant work experience in two or more of the 10 domains of the CISSP CBK (common body of knowledge), or four years of work experience and a four-year bachelor's degree or a master's degree in information security. To maintain the certification, CISSP holders are required to obtain 120 continuing professional education (CPE) credits every three years, with a minimum of 20 CPEs posted during each year of the three-year certification cycle. This continuing education ensures that CISSP-certified pros are keeping up with the latest threats."

Certification (GIAC) [14] offered by the SANS Institute.[15] While these successful existing cyber security certification programs provide models for the telecommunications industry, they do not fully address the uniqueness and complexity of the evolving telecommunications industry. A reasonable approach may be to offer telecommunications specific certifications as add-on concentrations under these current programs.

Security Policy Compliance: Tools, Interdependencies and Research Areas

As our telecommunications networks grow in scale, diversity and interconnection, there is a corresponding need for the development of efficient methods and tools to evaluate and assess the adherence of deployed network infrastructure to security requirements and policies. With the complexity of the networks, more work is needed to develop new and improved tools that can **automate** the management and analysis of security controls across the infrastructure. It is also worth recognizing that the use of powerful automated tools can have significant benefits that extend beyond security. Configuration assessment tools, for example, can improve network availability by identifying mis-configurations and inefficient system use and by reducing the labor cost of debugging and remediating mistakes.[16] Many of these tools rely upon the underlying capability to **specify**, in sufficient detail, security policies that can be translated into enforceable system configurations and rule sets. Current advances and research in specification languages, policy-based management, and cognitive networking are

[14] http://www.giac.org/

[15] http://www.sans.org/

[16] Telcordia has performed research, under Department of Homeland Security seed funding, to address the policy compliance problem across large packet-based networks. This research has led to a commercial product (i.e., IPAssure) that is complementary to configuration and system management tools on the commercial marketplace; see http://www.telcordia.com/products/ip-assure.

producing promising results for developing networks with much greater self-managing capabilities.

Telcordia has previously commented on the close and growing connections between telecommunications and electric power.[17] Telcordia believes the FCC's security initiative should consider its applicability for the emerging Smart Grid for power management, as well as other significant new broadband domains, and facilitate the elimination of any security gaps.

Proper sharing of risk information, especially key learnings, between commercial business partners and interconnected service providers is essential for smooth and secure telecommunications operations. There is value in the collection, assessment, and distribution of information and, more importantly, of knowledge gained from key learnings between skilled security practitioners. In the past, many of these key learnings were both technology related and procedural in nature. The NSTAC NSIE[18] has pioneered the sharing of information across vendors, providers and sectors. The evolving telecommunications environment will require more stakeholders to be active participants to reach a meaningful security baseline to meet the FCC's objectives.

Lastly, we believe that further security research to determine best practices for "building a trusted network from yet-to-be-trusted components" is necessary. This objective is at the core of securing the telecommunications infrastructure. It covers not just system and network security features previously discussed, but also the security of

[17] See Telcordia's responses to the National Broadband Plan Comment #8 on "Public Safety, Homeland Security and Cyber Security Elements," Public Notice DA 09-2133, submitted in November, 2009 and to the Notice of Inquiry on "Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload," PS Docket No. 10-92, submitted in June, 2010.

[18] Network Security Information Exchanges

the development and maintenance of the underlying products provided by global vendors. In turn, these vendors have their own supply chain of vendors providing components. Foreign supply chain risk management is a key tenet of the Comprehensive National Cybersecurity Initiative (CNCI).[19] NIST has recently published an approach to address these risks.[20] This risk management work needs to be expanded to address the downstream risks (e.g., software and firmware integrity) associated with building and deploying complex telecommunications networks. Basic research in this area could help to improve the security of the nation's telecommunication infrastructure.

[19] Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply chain Risk Management.

[20] Piloting Supply Chain Risk Management Practices for Federal Information Systems, Draft NISTIR 7622, June 2010.

CONCLUSION

Telcordia applauds the FCC's focus on cyber security improvements and encourages the FCC to continue to provide impetus and support to the telecommunications industry as it works through all of the difficult details of developing criteria and guidelines and designing programs that strike an appropriate balance. Telcordia urges the FCC to consider our comments and recommendations.

Respectfully submitted,

TELCORDIA

By: Deborah K Nord

Deborah Nordeen, Acting President
Advanced Technology Solutions
TELCORDIA
One Telcordia Drive
Piscataway, New Jersey
(732) 699-8013
dnordeen@telcordia.com

July 12, 2010